DETAILED ACTION

The instant application having Application No. 10/541422 filed on 4/27/06 is presented for examination by the examiner. The examination is based on the election restriction filed 10/20/2008. Examiner acknowledges Applicant's election of group 1. Claims 1-3, 6, and newly added 9 are present for examination on the merits.

Priority

Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been received.

Claim Objections

Claim 6 are objected to because of the following informalities: the phrase "insofar" is not generally present in US application. Examiner suggests a more traditional US terminology.

Claims 2 and 3 are objected to because they refer to their parent claim as "a method", instead of "the method". The latter form solidifies the relationship of the child to the parent claim by removing doubt as to whether it is similar to the parent or the same as the parent.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:
Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 1is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claim is directed to a judicial exception, namely an abstract idea because the claim does not require any physical transformation and the invention as claimed does not produce a useful, concrete, and tangible result. The claim seems to involve steps to manipulate digital data. There is no physical transformation being performed in the claim because transformation of data is not a "physical transformation". If there is not physical transformation there must be a useful, concrete, and tangible result. Examiner finds no tangible result stemming from the claim.

Dependent claims 2, 3, and 9 are likewise rejected under 35 USC 101 for the above mentioned reasons because they fail to rectify the deficiencies of claim 1.

Independent claim 6 is considered to not fail the statutory requirement of 35 USC 101 because a physical transformation to a computer is performed. Therefore the computer is physically changed by storing the software into its inherent hard disk drive of the hardware profile. And thus the claim provides a useful, concrete, and tangible result.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claim 9 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Claim 9 is a single means claim and does not appear in combination with the recited steps of claim 1. Furthermore, data analysis means covers all possible means for ways of analyzing data since it is not tied to any physical requirement and is not orderly connected to any of the steps in claim 1. See MPEP 2164.08(a).

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-3, and 9 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 1, the phrase "executable protection software portion" has a dual interpretation which renders the claim indefinite. The question is raised whether there exists some additional portion of an executable protection software or is this part of the secure wrapper. And secondly if this is a "first" portion is there a connection to an

unknown second portion? The same ambiguousness is present by the term "a specific performance portion. The word portion causes the relationship between the wrapper, and the executable protection software to become blurred.

The phrase "software and development platform" is indefinite because the word "*and*" introduces the question of whether said phrase is one entity or two entities. If said phrase is one entity a hyphen would be more appropriate than the word *and*. Appropriate correction is required.

Claims 2, 3, and 9, are likewise rejected for failing to rectify the above mention deficiencies.

As per claim 2, the phrase "whether an operating system is operative having multiple virtual storage" is awkward and possibly missing some words so that the phrase makes sense. Examiner cannot ascertain the intent of this phrase. However for reason of examination, Examiner will give it the broadest reasonable interpretation and assume it means the operating system can operate on a virtual storage. Having the word multiple beside a singular storage is confusing.

Claim 3 is indefinite because it is unclear what constitutes registration. The claim calls for decryption when the some unclearly specified entity is registered.

Claim 9 is indefinite because it is unclear how and when the step of providing data analysis is performed in conjunction with the method of claim 1.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 6, and 9 are rejected under 35 U.S.C. 102(b) as being anticipated by USP 6,243,468 to Pearce et al., hereinafter Pearce.

As per claim 1, Pearce teaches a method of monitoring digital information (col. 2, lines 35-40) including: creating a secure wrapper [associate product ID] around the digital information [software product] using a method selected from: a first wrapper method including directly embedding a first executable protection software portion [registration pilot, col. 6, lines 30-31] in the digital information; or a second wrapper method including linking a second executable protection software portion to the digital information by way of an application program interface (API); or a third wrapper method including modifying the digital information and embedding a third executable protection software portion in the modified digital information; each of the first, second and third executable protection software portion including a specific performance portion operable by a user to perform one or more specific performance tasks [call service rep. and enter registration ID, col. 6, lines 32-33], the one or more specific performance tasks including a hardware environment check [checking hardware ID, col. 6, lines 40]; selecting one of the first second or third wrapper methods according to a software and development

platform associated with said digital information [notion of putting the protective software on the software product], the accessibility of the source code of the digital information, or the level of monitoring required; executing [registering] the selected wrapper (col. 5, lines 40-41) method by way of the first, second or third executable protection software portions including the steps of; intercepting access to the digital information [registers software during installation, col. 5, lines 45-46); checking that at least one of the one or more specific performance tasks has been performed (col. 6, lines 64-68), including that said hardware environment check [hardware ID] has been performed; and validating whether or not the hardware environment corresponds to the hardware environment which has been previously checked (col. 7, lines 1-10).

As per claim 6, Pearce teaches a method of protecting software, the method insofar as the installation and registration (col. 5, lines 40-41) of the software including the steps of: installing the software on a computer having a hardware profile (col. 5, lines 30-31); after installing the software, running the software for a first time (col. 5, lines 44-45); upon the running of the software on the computer, generating an installation code from said hardware profile of the computer (col. 5, line 58); after generating the installation code, requesting a unique serial number from an authorization source [registration server, col. 6, lines 36-39), the request including providing said hardware profile [hardware ID] of the computer; after requesting the serial number [product ID], registering the software with a registration authority using an obtained serial number and said installation code; receiving a positive or negative reply from the registration authority (col. 6, lines 39-43); upon the receipt of a negative reply

from the registration authority, returning to the step of requesting a serial number and following the steps thereafter [blocks access until registration is performed successfully]; upon the receipt of a positive reply from the registration authority, receiving a registration key [Reg ID] from the registration authority and saving the registration key on the computer (col. 6, lines 37-39), whereupon the software may be executed insofar as its functional performance is concerned; the

method insofar as the post-registration running of the software including the further steps of: running the software on the computer; upon the running of the software on the computer, generating an installation code from the hardware profile of the computer; after the hardware profile has been generated, comparing the registration key with the hardware profile; upon the matching of the hardware profile with the registration key, permitting the software to executed insofar as its functional performance is concerned; upon the failure of the hardware profile to match the registration key, denying permission for the software to executed insofar as its functional performance is concerned (col. 5, line 59-col. 6, line 12).

As per claim 9, Pearce teaches providing data analysis means for analyzing the registration, usage or other billing, behavioral, demographic or market analysis of the digital information [registration is analyzed by revealing which product keys have been used and further making sure the same product key has not been registered on different hardware, col. 3, lines 1-4).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:
(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Pearce in view of USP 6,891,953 to DeMello et al., hereinafter DeMello.

As per claim 2, Pearce is silent in performing the security checked based on a user's account in addition to the hardware environment when the operating system is operating with virtual storage. Microsoft operating systems as taught by Pearce inherently use virtual memory. DeMello teaches when a software product is being registered, in addition to the hardware profile, a user's digital passport is attached and embedded in the user's PC, thus tying not only the machine but the user to the licensed software product (col. 24, lines 4-40). This effectively allows a single user the ability to register the software on multiple computers if allowed by the licensor while preventing the chance of the user giving his/her software program to others and having them register their copy on their own hardware. In this case it would be an improvement over Pearce's system because it adds flexibility to the system while maintaining security. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teaching of Pearce with the teaching of DeMello because it

would improve the systems able to safeguard its licenses while yielding more flexibility to the user.

Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Pearce in view of USP 7,330,978 to Harrington et al., hereinafter Harrington.

As per claim 3, Pearce teaches the said digital information is in the form of a non-executable, browser-readable code or content [software program is content, col. 2, lines 35-40). Pearce is silent in teaching creating a mapping table capable of translating and preserving text, object paths, and extensions within a single container or file structure to form a mapped file; converting the mapped file into an executable file structure to form a conversion file; and encrypting the conversion file to form an encrypted file to enable dynamic decryption of selected content of the encrypted file when correctly registered. These steps are essentially taking content placing it into an executable file also known as an installation file and encrypting it. Decryption is only allowed once it is registered. It is notoriously well-known to take a software program and place all of its files and folders into an installer executable on the Windows™ platform. Harrington teaches encrypting that installer until it is registered thus denying a user even the chance of extracting any useful material from the software because it is contained in a single encrypted file (col. 1, lines 60-66). It is obvious to combine the use of a known technique to improve similar methods in the same way. The claim would have been obvious because encrypting installers for security was part of the ordinary capabilities of

a person of ordinary skill in the art.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure is listed on the enclosed PTO-892 form.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./
Examiner, Art Unit 2431
/Syed Zia/
Primary Examiner, Art Unit 2431